UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

KIA MACKEY, individually and on behalf of all others similarly situated, Plaintiff, v. BELDEN, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kia Mackey ("Plaintiff" or "Plaintiff Mackey"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class members" as defined below) and by and through her undersigned counsel, files this Class Action Complaint against Defendant Belden, Inc. ("Belden" or "Defendant") and alleges the following based upon personal knowledge of facts pertaining to herself and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused her and the other Class members in the large and preventable data breach that was discovered by Belden on November 12, 2020 and announced publicly by Belden on November 24, 2020, in which unauthorized users accessed Belden servers that contained personal information of current and former employees and business partners ("Data Breach" or "Breach").[1]

2. Grass Valley USA, LLC ("Grass Valley"), a former subsidiary of Belden, was made aware of the Data Breach on November 18, 2020. According to the Notice of Data Incident

[1] *See* Notice of Data Breach provided to California Attorney General, attached hereto as **Exhibit 1.**

disseminated by Belden, Grass Valley was owned by Belden until July 2020. Belden continues to provide IT, HR and other services for Grass Valley pursuant to the terms of Grass Valley's divestiture.[2]

3. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, some companies still fail to put adequate security measures in place to protect their customers' and employees' data.

4. Defendant, a provider of networking, connectivity, and cable products, which designs, manufacturers, and markets signal transmission products for applications, is among those companies which have failed to meet its obligation to protect the sensitive personal identifying information entrusted to them by current and former employees, or current and former employees of Belden's subsidiaries[3].

5. Belden has not yet disclosed when the Data Breach occurred, but on November 24, 2020, it announced that an unknown third party gained unauthorized access to its servers that were used to store certain employee data. Data including names, birthdates, government-issued identification numbers (e.g. Social Security numbers), bank account information (for North American employees on Belden/Grass Valley payroll), home addresses, email addresses, and other general employment-related information ("PII") was accessed.

6. As a corporation doing business in Missouri, Defendant is legally required to protect the PII it gathers from unauthorized access and exfiltration.

---

[2] *Id.*

[3] Unless specified otherwise, "employee" as used herein includes former and current employees of Belden or any of its subsidiaries as well as Belden business partners.

7. As a condition of employment, Plaintiff and the Class members were required to disclose their PII to Defendant, entrusting Defendant to keep it safe and protected.

8. Defendant collected its employees' sensitive PII. And in acquiring various subsidiaries, Defendant collected the PII of employees of those businesses. In either case, Defendant had an obligation to secure that PII by implementing reasonable and appropriate data security safeguards.

9. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiff's and the Class members' PII has been exposed to those who should not have access to it. Plaintiff and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly sensitive PII stolen here.

THE PARTIES

10. Defendant Belden, Inc., is a Delaware corporation with its principal place of business in St. Louis, Missouri. Belden is a provider of networking, connectivity, and cable products and conducts business worldwide. Belden was founded in 1902 and is one of the largest U.S.-based manufacturers of high-speed electronic cables primarily used in industrial, enterprise, and broadcast markets. Now, with thousands of current and former employees, Belden's estimated annual revenues exceed $2 billion.

11. Plaintiff Kia Mackey is a resident of Indianapolis, Indiana. In December 2020, Plaintiff received notice from Belden by letter dated December 11, 2020 that it improperly exposed her PII to unauthorized third parties. Plaintiff worked for Belden from 2019-2020.

12. Plaintiff reasonably believed Defendant would keep her PII secure. Had Defendant disclosed to Plaintiff that her PII would not be kept secure and would be kept easily accessible to hackers and third parties, she would have taken additional precautions relating to her PII.

13. As a result of the Data Breach, unknown, unauthorized cyber criminals used Plaintiff's PII to attempt to file a tax return via Turbo Tax using Plaintiff's Social Security number and an old address at which she lived when she was a Belden employee.

14. Plaintiff received notice of the fraudulent attempt via an email from Turbo Tax on January 15, 2021.

15. Plaintiff has spent hours responding to the Data Breach, including verifying through various methods that the notice from Turbo Tax was legitimate and not a phishing attempt itself, resulting in her speaking directly with an Intuit/Turbo Tax employee who confirmed that someone had utilized her PII in attempts to file a fraudulent tax return.

16. Plaintiff spent and continues to spend additional time reviewing her credit monitoring service results and reports from other online resources concerning the security of her identity and financial information.

17. Plaintiff suffered actual injury from having her PII exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of her PII—a form of intangible property that the Plaintiff entrusted to Belden as a condition of her employment; (b) loss of her privacy; and (c) imminent and impending injury arising from the increased risk of additional fraud and additional identity theft.

JURISDICTION AND VENUE

18. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one Class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in Missouri, and has sufficient minimum contacts with Missouri.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

21. Application of Missouri law to this dispute is proper because Defendant's headquarters are in Missouri, the decisions or actions that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in Missouri, and the action and/or inaction at issue emanated from Missouri.

FACTUAL ALLEGATIONS

A. Defendant collects and stores thousands of current and former employees' PII and fails to provide adequate data security

22. Belden was founded in 1902 and has evolved over the years through many mergers and acquisitions to be a major international corporation. It has had many subsidiaries, including Grass Valley USA, LLC.

23. Currently, Belden is a publicly traded company with annual revenue totaling more than $2 billion in 2019. It is a major player in the industry. In addition to a full range of cable manufacturing, Belden manufactures fiber and copper connectors and networking products such as Ethernet switches. Its products are used in industrial, enterprise, broadcast, and consumer electronics applications. Belden has more than 8,000 employees and thousands of former employees and has grown by acquiring other companies, including those that employed certain Class members.

B. Belden's inadequate data security exposes its employees' sensitive PII

24. On an unknown date prior to November 12, 2020, unknown third-party cyber criminals gained access to a Belden server that was used to store employee data.

25. Employee names, birthdates, government-issued identification numbers (e.g. Social Security numbers), bank account information (for North American employees on Belden/Grass Valley payroll), home addresses, email addresses, and other general employment-related information was among the PII that may have been accessed by the hackers.

26. Plaintiff received a letter from Belden dated December 11, 2020 entitled "Notice of Data Incident." The letter stated that her PII, detailed below, may have been compromised, and included the following information:

> **What Happened?**
>
> On the evening of November 12, 2020, Belden IT professionals detected unusual activity involving certain company servers. We immediately triggered our cybersecurity incident response plan, deployed teams of internal IT specialists, and engaged leading third-party cybersecurity forensic experts and other advisors to identify the scope of the incident and move quickly to mitigate the impact. Forensics experts determined that we were the target of a sophisticated attack by a party outside the company. On or about November 15, 2020, we learned that the outside party accessed servers that contained personal information of some current and former employees.
>
> **What Information Was Involved?**
>
> The personal information involved in this incident may have included your name, birthdate, government-issued identification numbers (for example, social security number), bank account information (for North American employees on Belden payroll), home addresses, email addresses and other general employment-related information.
>
> **What Are We Doing?**
>
> While our investigation continues, we believe that we have stopped further access of personal data on our servers. We are also working with regulatory and law enforcement officials, including the F.B.I. and Department of

> Homeland Security, to investigate the matter and have engaged legal counsel to help us notify appropriate regulatory authorities. In addition, we are continuously monitoring for any suspicious activity on our systems and have deployed additional resources to reinforce the security of our systems.

C. It is well established that data breaches lead to identity theft and other harms

27. Plaintiff and Class members have been injured by the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use and/or viewing of their PII as a result of the Data Breach.

28. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[4] With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: opening new financial accounts in the victim's name, taking out loans in the victim's name, obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[5]

29. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell and trade the information on the cyber black-market for years.

---

[4] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Oct. 30, 2020).

[5] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Oct. 30, 2020).

30. This is not just speculative. As the FTC has reported, if hackers get access to PII, they ***will*** use it.[6]

31. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[7] Identity thieves can also use the information stolen from Plaintiff and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

32. If, moreover, cyber criminals also manage to acquire financial information, credit and debit cards, health insurance information, driver's licenses and passports, there is no limit to the amount of fraud to which Defendant has exposed Plaintiff and Class members.

33. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[8] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[6] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Oct. 30, 2020).

[7] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 30, 2020).

[8] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 30, 2020).

34. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[9]

35. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

36. There may be a time lag between when sensitive PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

37. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various Internet websites making the information publicly available.

38. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[11]

39. Defendant's failure to adequately protect Plaintiff's and Class members' PII has resulted in Plaintiff and Class members having to undertake mitigation tasks, which require

---

[9] *Id.* at 2, 9.
[10] *Id*. at 29 (emphasis added).
[11] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Oct. 30, 2020).

extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money.

40. Defendant's offer of twenty-four months of identity monitoring and identity protection services to Plaintiff and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[12] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

41. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, substantial and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

42. Plaintiff and the Class members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

[12] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Oct. 30, 2020).

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their PII used against them by spam callers, texters, and emailers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' PII, for which there is a well-established and quantifiable national and international market;

i. Damage to their credit due to fraudulent use of their PII; and/or

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

43. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

44. Defendant itself acknowledged the harm caused by the Data Breach by offering Plaintiff and Class members twenty-four months of identity theft monitoring services and identity protection services. Twenty-four months of identity theft monitoring and identity protection services is woefully inadequate to protect Plaintiff and Class members from a lifetime of identity

theft risk and does nothing to reimburse Plaintiff and Class members for the injuries they have already suffered.

D. Belden failed to comply with Federal Trade Commission requirements

45. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[13]

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[14] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

47. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security;

---

[13] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 6, 2020).

[14] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last October 6, 2020).

[15] *Id.*

monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

48. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[17]

49. By allowing an unknown third party to access a Belden server, Belden failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Belden's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff and the Class members suffered damages

50. The ramifications of Defendant's failure to keep current and former employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[18]

51. The PII belonging to Plaintiff and Class members is private, sensitive in nature, and was left inadequately protected by Defendant, who did not obtain Plaintiff's or Class members'

[16] Federal Trade Commission, *Start With Security*, *supra* note 5.
[17] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited October 6, 2020).
[18] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Nov. 11, 2020).

consent to disclose such PII to any other person as required by applicable law and industry standards.

52. The Data Breach was a direct and proximate result of Belden's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

53. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately implement data security measures, despite its obligations to protect current and former employees' PII.

54. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of PII.

55. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have already experienced and are at continuing risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

56. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more

resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

57. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

58. In addition to a remedy for the economic harm, Plaintiff and the Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

---

[19] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Nov. 11, 2020).

F. Belden's delay in identifying and reporting the breach caused additional harm

59. While it is still unknown when the breach occurred, affected current and former employees were not notified of the Data Breach until November 24, 2020 or later and are unaware of how long their PII has been exposed to cyber criminals, thus depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

60. As a result of Belden's potential delay in detecting and notifying current and former employees and business partners of the Data Breach, the risk of fraud for Plaintiff and Class members has been driven even higher.

CHOICE OF LAW

61. Defendant is headquartered in Saint Louis, Missouri. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

62. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's Missouri headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in Missouri. Finally, Defendant's breach of its duty to employees—including Plaintiff and Class members—emanated from Missouri.

63. It is appropriate to apply Missouri law to the claims against Defendant in this case due to Defendant's significant contacts with Missouri. Defendant is headquartered in Missouri; the relevant decisions, actions, and omissions were made in Missouri; and Defendant cannot claim to be surprised by application of Missouri law to regulate its conduct emanating from Missouri.

64. To the extent Missouri law conflicts with the law of any other state that could apply to Plaintiff's claims against Defendant, application of Missouri law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

CLASS ACTION ALLEGATIONS

65. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who are employees or former employees, or business partners, of Belden or any of its affiliates, parents, or subsidiaries, who had their PII compromised as a result of the Data Breach that was publicly announced on November 24, 2020.

66. In addition, Plaintiff brings this action on behalf of herself and the following proposed Indiana subclass defined as follows:

> All persons residing in the State of Indiana who are employees or former employees, or business partners, of Belden or any of its affiliates, parents, or subsidiaries, who had their PII compromised as a result of the Data Breach that was publicly announced on November 24, 2020.

67. Both the proposed National Classes and the proposed Indiana subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

68. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Belden; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

69. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

70. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein,

b. Whether Defendant's inadequate data security measures were a cause of the data security breach,

c. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII,

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII,

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the data security breach,

f. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class members' PII in violation of Section 5 of the FTC Act,

g. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

h. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

71. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

72. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner.

73. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

74. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Class)

75. Plaintiff incorporates paragraphs 1 through 74 as though fully set forth herein.

76. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class members' PII in Defendant's possession was adequately secured and protected.

77. Defendant owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of its current and former employees.

78. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees and the critical importance of adequately securing such information.

79. Plaintiff and members of the Class entrusted Defendant with their PII with the understanding that Defendant would safeguard their information, would not store the information longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

80. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach.

81. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses in the United States.

82. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class members.

83. Because Defendant knew that a breach of its systems would damage thousands of current and former Belden employees, and business partners of Belden, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

84. Defendant had a special relationship with Plaintiff and Class members by virtue of their being current employees, former employees, or business partners. Plaintiff and Class members reasonably believed that Defendant would take adequate security precautions to protect their PII.

85. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' PII.

86. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members during the time it was within Defendant's possession or control.

87. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third-party hacker to access a Belden server containing current and former employee

PII, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect its current and former employees' PII.

88. Plaintiff and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiff and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent. As a result, Defendant is negligent per se.

89. Neither Plaintiff nor the other Class members contributed to the Data Breach as described in this Complaint.

90. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and

continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

91. Plaintiff incorporates paragraphs 1 through 90 as though fully set forth herein.

92. Defendant offered employment to the current or former employee Plaintiff and Class members, either directly or through acquiring the businesses for which Plaintiff and Class members worked, in exchange for compensation and other employment benefits. Belden also formed relationships with business partners in exchange for compensation. Defendant either required Plaintiff and Class members to provide their PII or acquired their PII from their former employers which Defendant acquired, including names, addresses, dates of birth, Social Security numbers, bank account information, email addresses, and other personal information. Defendant also obtained private information related to its business partners.

93. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

94. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure and/or use.

95. Plaintiff and Class members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

96. Plaintiff and Class members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead

retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

97. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII.

98. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered injury as described in detail in this Complaint and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiff and the Class)

99. Plaintiff incorporates paragraphs 1 through 98 as though fully set forth herein.

100. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant.

101. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

102. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

103. Defendant voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

104. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

105. As a direct and proximate result caused by Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages.

106. But for the unauthorized disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

107. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of the unauthorized disclosure of Plaintiff's and Class members' PII. Defendant knew its computer systems and technologies used for accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class members' PII in jeopardy.

108. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach,

including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of Plaintiff and the Class)

109. Plaintiff incorporates paragraphs 1 through 108 as though fully set forth herein.

110. Missouri established the right to privacy in Article 1, Section 15 of the Missouri Constitution.

111. Under Missouri law, the right of privacy is invaded when there is "(1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public." *Sofka v. Thal*, 662 S.W.2d 502, 510 (Mo. banc 1983).

112. Plaintiff and Class members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

113. Defendant owed a duty to its employees, including Plaintiff and Class members, to keep their PII confidential.

114. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the type of information that is the subject of this action, is highly offensive to a reasonable person.

115. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendant as part of their employment with Defendant, but privately, with the intention that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

116. The Data Breach constitutes an unreasonable intrusion upon Plaintiff's and Class members' seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

117. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

118. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

119. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class members to suffer damages.

120. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendant can be accessed by, acquired by, appropriated by, disclosed

to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

121. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class members. As such, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class)

122. Plaintiff incorporates paragraphs 1 through 121 as though fully set forth herein.

123. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees, including Plaintiff and Class members. This duty included the obligation to safeguard Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

124. Defendant further breached its fiduciary duties owed to Plaintiff and Class members as former employees by failing to remove and otherwise destroy Plaintiff's and Class members' PII from Defendant's systems, as Defendant's employment relationship had ceased and Defendant no longer had any valid purpose for the maintenance and storage of that data.

125. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to properly encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class members' PII. Defendant further breached

its fiduciary duties owed to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

126. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

127. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses. As such, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Class)

128. Plaintiff incorporates paragraphs 1 through 127 as though fully set forth herein.

129. As described above, when Plaintiff and the Class members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect their PII and to timely notify them in the event of a data breach.

130. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

131. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations when it engaged in unlawful practices under other laws. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class members' PII; storing the PII of former employees despite any valid purpose for the storage thereof ceasing upon terminating the relationship with those individuals; and failing to disclose to Plaintiff and Class members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

132. Plaintiff and Class members did all or substantially all the significant things that the contract required them to do.

133. Likewise, all conditions required for Defendant's performance were met.

134. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class members' rights to receive the full benefit of their contracts.

135. Plaintiff and Class members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

136. Defendant is liable for this breach of these implied covenants whether or not it is found to have breached any specific express contractual term.

137. Plaintiff and Class members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses, in amounts to be determined at trial

SEVENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiff and the Class)

138. Plaintiff incorporates paragraphs 1 through 137 as though fully set forth herein.

139. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

140. As previously alleged, Plaintiff and Class members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class members.

141. Defendant owes a duty of care to Plaintiff and Class members requiring it to adequately secure PII.

142. Defendant still possess PII regarding Plaintiff and Class members.

143. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

144. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

145. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

146. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

147. Plaintiff, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and

ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring,

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems,

e. Ordering that Defendant not transmit PII via unencrypted email,

f. Ordering that Defendant not store PII in email accounts,

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services,

h. Ordering that Defendant conduct regular computer system scanning and security checks,

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

EIGHTH CAUSE OF ACTION
Violation of the Indiana Deceptive Trade Practices Act
IC §§ 24-5-0.5-1, *et seq.*
(On behalf of Plaintiff and the Indiana Subclass)

148. Plaintiff incorporates paragraphs 1 through 147 as though fully set forth herein.

149. Defendant violated the Indiana Deceptive Trade Practices Act (IC §§24-5-0.5-1, et seq.) by failing to prevent Plaintiff's and Indiana Subclass members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and Indiana Subclass members.

150. Defendant is a "supplier" pursuant to IC §§24-5-0.5-2(a)(3) that engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to employment services in Indiana, including but not limited to the following:

a. Defendant mispresented material facts by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Indiana Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Defendant misrepresented material facts to Plaintiff and the Indiana Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Indiana Subclass members' PII;

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Indiana Subclass members' PII;

d. Defendant engaged in deceptive, unfair and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and Indiana Subclass members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. §45) and Indiana's data breach statute (IC §24-4.9-3.5); and

e. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and Indiana Subclass members in a timely and accurate manner, contrary to the duties imposed by IC §24-4.9-3.3.

151. Plaintiff and the Indiana Subclass members are considered "consumers" pursuant to the Indiana Deceptive Trade Practices Act, and their employment with Defendant constituted a "consumer transaction" in that it consisted of services provided (IC §§24-5-0.5-2(a)(1)).

152. Defendant violated the Indiana Deceptive Trade Practices Act, IC §§24-5-0.5-1, et seq., when it engaged in fraudulent and deceptive conduct that created a likelihood of confusion and misunderstanding by assuring Plaintiff and the Indiana Subclass members that their PII would be kept safe and unobtainable from unauthorized third persons.

153. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute an "incurable deceptive act" pursuant to IC §§24-5-0.5-2(a)(8).

154. As a direct and proximate result of Defendant's acts, Plaintiff's and the Indiana Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

155. As a direct and proximate result of Defendant's acts, Plaintiff and the Indiana Subclass members were injured and lost money or property, including but not limited to the loss of Plaintiff's and the Indiana Subclass members' legally protected interest in the confidentiality and privacy of their PII, damages, and additional losses as described above.

156. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Indiana Subclass members' PII and that the risk of a data breach or theft was high. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the Indiana Subclass members.

157. Plaintiff and Indiana Subclass members seek relief under IC §§24-5-0.5-4, including, but not limited to, recovery of actual damages or $500.00, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs (pursuant to IC §24-5-0.5-4). Senior members of the Indiana Subclass also seek treble damages, pursuant to IC §24-5-0.5-4(i).

158. Plaintiff and the Indiana Subclass members also seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Plaintiff's and the Indiana Subclass members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Plaintiff's and the Indiana Subclass members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated and the Class, respectfully requests the Court order relief and enter judgment in their favor and against Belden as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein.

B. Plaintiff requests injunctive and other equitable relief as is necessary to protect the interests of the Class, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering it to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendant to implement multi-factor authentication requirements; (viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Defendant to encrypt all PII; (x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; (xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII no longer necessary for the provision of services; (xiii)

requiring Defendant to conduct regular computer system scanning and security checks; (xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members; and (xvi) requiring Defendant to educate all Class members about the threats they face as a result of the loss of their PII to third parties, as well as steps Class members must take to protect themselves.

C. A judgment awarding Plaintiff and Class members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendant pay the costs involved in notifying the Class members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: February 4, 2021

Respectfully submitted,

DANNA McKITRICK, P.C.

By: *s/Jeffrey R. Schmitt*

Jeffrey R. Schmitt, #52966MO
Katherine M. Flett, #68183MO
7701 Forsyth Blvd., Suite 1200
St. Louis, MO 63105
(314) 726-1000 / (314) 725-6592 (fax)
E-mail: jschmitt@dmfirm.com
kflett@dmfirm.com
Counsel for Plaintiff and the Putative Class

s/William B. Federman

William B. Federman, OBA #2853*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com
Counsel for Plaintiff and the Putative Class
**Pro hac vice application forthcoming*